J.C. Buitelaar

ID Number policies in Europe

Der Beitrag liefert einen Überblick über die konzeptionellen, historischen, soziologischen und technischen Implikationen einer Politik der Identifizierungsnummern zwischen funktionalen Verwendungsinteressen einerseits und dem Datenschutz andererseits. Der Beitrag prognostiziert unterschiedliche Identifikatoren für verschiedene Verwendungszwecke, die interoperabel sein können, aber auch gleichzeitig eine Steuerung durch den Nutzer ermöglichen.

Abstract

The objective of this article is to present a view on the sensible use of the identification numbers, especially in the public domain. The question of whether proper use can be achieved by a single global identifier or multiple identifiers will be answered.

In the report on which this article is based, several FIDIS partners investigated different aspects of ID numbers, such as the history of the use of identification documents, the legal framework, the sociological theoretical aspects and the possible use of ID numbers in the technique of profiling. Thus the investigations presented in the report provided a sound basis for determining the risks and opportunities in using ID numbers, especially in the area of e-government.

From a European point of view the choices made of using either a single global identifier or multiple identities, are illustrated. The report shows how the ID number can be put to good use while at the same time not unduly harming the privacy interests of the individual.

Drs J.C. Buitelaar MA, TILT

Universität Tilburg, Fachbereich Rechtswissenschaft. Mitglied des europäischen fidis-Netzwerkes (Future of Identity in the Information Society)
E-Mail: J.C.Buitelaar@uvt.nl

1 Introduction

Within the Fidis (Future of Identity in the Information Society) network of excellence a study has been made of identification number policies across Europe.[1] The study is part of the analysis of the implications of technologies for protecting and enabling the secure and trusted distribution of identity digital assets.

Much discussion takes place about the desirability of a single identification number in the context of eGovernment development. This is a matter of a fundamental nature. It goes without saying that personal identification forms an important part of the foundation of our society. It allows us to create a link between people, actions and responsibilities. In many ways it is one of the lubricants which allow society to function.[2]

Whereas in the past, physical means of identification predominated, we are now on the eve of an era where digital equivalents of these forms of identification will take over.[3] Without these measures, fighting crime will be obstructed, ambitions in the field of eGovernment will be frustrated, companies and citizens will lack faith in e-commerce, to name but a few things that could go wrong.

Careful attention to the design of the system of digital identification is essential. It may be fair to state that it is doubtful whether there is sufficient consideration of the advantages and disadvantages of the use of an identification number, without which, a digital identification system cannot function.[4]

Being part of the broader Fidis network of excellence it is therefore worthwhile to analyse several crucial aspects of the policies which might lead to enabling secure and trusted distribution of identity digital assets. A historical analysis is provided in an attempt to make clear the background against which political choices in several European countries are made concerning the framework within which ID numbers are distributed. It goes without saying that the legal aspects of the use of digital identification need close scrutiny.

After all ID numbers are personal data and therefore the European Data Directive might be expected to offer a firm basis for a proper use of the ID number. Even though it might seem that ID numbers are a mere technical matter for which a proper legal basis is present, it turns out that this legal basis is soon set aside for technical priorities and managerial advantages.

In order to understand why the general public quite often – as was shown in the historical chapter has felt an almost instinctive need to oppose the general introduction of such a number, a sociologial

1 Buitelaar, H. (ed.), D13.3: Study on ID number policies, FIDIS deliverable, 2007. Gratitude is due to the main contributors to the study: Marita Häuser, Martin Meints, Martin Rost, Unabhängiges Landeszentrum für Datenschutz (ICPP), Kiel, Mireille Hildebrand, Erasmus Universiteit Rotterdam and Vrije Universiteit Brussel, Xavier Huysmans, Katholieke Universiteit Leuven (ICRI), Isabelle Oomen, Universiteit van Tilburg (TILT)..

2 Prins, C. and de Vries, M., ID or not to be? Naar een doordacht stelsel voor digitale identificatie [ID or not to be? Towards a well thought out system for digital identification], Rathenau Instituut, Working document 91, den Haag, 2003, p. 13.

3 College bescherming persoonsgegevens, Electronische overheid en privacy. Bescherming van persoonsgegevens in de informatiestructuur van de overheid, Den Haag, 2002.

4 Koops thinks the time is ripe for a reconsideration because once the information society is there it cannot be turned back. Koops, B.J., 'Een nieuwe GBA, digitale kluisjes en identificatiedrang', [A new GBA, digital vaults and the identification urge], NJB, vol. 32 (32), 2001, pp. 1555-1561.

analysis pinpoints some of the reasons for these sometimes irrational emotions. The article concludes with a technical chapter, which offers some hope, that exactly the boundless surge of claims that technology makes to create this ideal world of eGovernment, will help in putting the digital identity number to good use with due respect for the privacy of the citizens concerned.

It can be stated that means of identification increasingly pervades the public sector. They originated in distinct areas of the public sector. Examples are taxation, public health, law-enforcement, local administrations and social services.

In the light of attempts to streamline government operations by making systems interoperable and in fighting fraud and terrorism, different developments can be witnessed in various EU countries. The various solutions proposed, offer different benefits and pose different threats to both governments and citizens.

The most eye-catching solution in this respect is the introduction of a single personal identification number to be used throughout the public sector. Undoubtedly, the advantage in reducing the administrative burden for both government and citizen makes the single identification a very attractive proposition. At the same time, the costs of security measures to safeguard it, may not be sufficient to retain the citizen's trust in a reliable government.

In the scenario, where substantial user control is absent, the introduction of a unique identifier makes the consumer and citizen more transparent. Facilitating the linkage of a profile to the number ID and linking different profiles to each other via this number, could potentially result in undesirable surveillance opportunities.

2 Historical approach

To be able to identify individuals in a reliable way always has been of importance, especially in the context of social groups (e.g. clans) and later in the context of States. This need typically covered all phases of human life, from birth to death. The context for identification always has been the determination of membership or non-membership in a group, a clan or State, and the regulation of access to resources, ownership or participation in this context.

In early societies such as the Greek Polis, identification was done by inspection. Societies were not very large, so every citizen knew every other citizen of his Polis in person.

This situation changed dramatically already in the Roman Empire. From time to time Roman Emperors tried to count their citizens using a census, as reported for example in the Bible (e.g. by the evangelist Luke in chapter 2.1). The census information was important to calculate taxes, the number of slaves and the number of possible soldiers. A census did not provide a means for identification of individual citizens.[5]

Somewhat later another practice became common: the use of travel documents for individuals. Typically these documents were used for persons with a special status such as rich citizens and noblemen. These travel documents typically were documents for passing through an area: visa or letters of recommendation. The purpose of these documents was to reduce the risks of travelling.

This was accomplished by a certificate of a reference person (typically a person of high status that was widely known) that the travelling person travelled for legitimate reasons, was trustworthy and worth being protected and supported on the journey by local authorities.

Taking in criminals on the other hand, was supported by using warrants of apprehension. They included a detailed description of the person searched for, the so called "signalement", and were copied many times after printing of books was developed.[6]

After the reformation the Catholic Church needed to know – among other things for tax reasons – how many members belonged to it. To facilitate this, the Council of Trent decided in 1563 that priests should write lists of persons who were baptised and married, and later also of those who were confirmed and buried. From the perspective of the Catholic Church this information was most important as it showed the real identity of a member of the church. Through baptism people became members of the church, a Christian marriage was important for a Christian life of couples and families, and a Christian burial also was very important.

This way of showing the identity of the church member, helped in guaranteeing that a person could be resurrected from death with a complete body, despite illness, wounding and death in his physical life.[7]

In 1796 Fichte stated that citizens needed to be detectable for public authorities at any time. For this purpose he suggested the introduction of a passport for every citizen, which precisely describes the passport holder.

Pursuing the same target, Jeremy Bentham suggested in 1843 that every citizen should bear a unique name. This name should be noted in a citizens' register and also should be tattooed on the wrist of the corresponding citizen. This permanent link between a physical person and a name certified by public authorities would strengthen the law and result in the disappearance of many criminal activities, Bentham claimed. In addition the identification would support prosecution in case of criminal actions.[8]

The French Revolution led, among other things, to the introduction of the "Code Civil" as civil law on 20th of September 1792. Because of the resulting modern understanding of citizenship, citizens' registers were run by the State instead of the churches. Identification of citizens of the State was based on a paper-based ID document together with an appropriate entry in the citizens' register by public authorities.[9]

The reintroduction of ID documents that were terminated earlier in the French Revolution resulted in a dilemma that was quite typical for the 19th century. On the one hand increasing liberalisation required free movement without passports standing in the way. On the other hand in times of real or perceptible crises, inner security (today often called homeland security) became a bigger issue and thus regis-

5 By the time of the Emperor Augustus, 30BC to 14AD, censuses were taken every 5 years. The Censor was an important public position in Rome. The census was also about taxation potential.

6 Groebner, V., *Der Schein der Person*, München, 2004.

7 Brockhaus, Konversationslexikon, Leipzig, 1898.

8 Caplan, J., 'This or that Particular Person', in: Caplan, J and Torpey, Documenting individual identity, Princeton, 2001; Cf de Hert, P., 'Jeremy Bentham on the need for identification by governments', in Koops, B.J., Buitelaar, H. and Lips, M. (eds), D5.4, Anonymity in electronic government: a case-study analysis of governments' identity knowledge, FIDIS Deliverable, 2007.

9 Groebner, V., *Der Schein der Person*, München, 2004.

tration of citizens and foreigners together with issuing ID documents was undertaken regularly.

But the target of effective administrative control in practice was seldom achieved due to putting off implementation of identifying measures. Noblemen typically did not need any ID documents, while normal citizens needed them as soon as they were leaving the county where they were living. Foreign travellers in addition had to keep strictly to a prescribed route and faced in addition numerous controls on their way.

De facto migration started to be a serious issue already in the 19th century. Millions of people moved around without any passport, changing effectively the demographic, political and economic landscape of Europe.

But ID documents also became important in another context in the 19th century. Police forces throughout Europe had introduced registers of poor people and of people that were moving around such as beggars, crippled people, veterans from various wars, prostitutes, lepers and showmen.

Security of the local population was a motivating factor for this registration, but different treatment of the local bereaved persons compared to moving poor people also was an issue. Based on the right of people at home the local poor population got better support (e.g., food and housing) compared to other groups. In any case to receive grants, people had to identify themselves using ID documents.[10]

When States in Europe changed from absolute monarchies to constitutional States in the 19th century, the relationship between State and its citizens changed. Passports (pass from the French term passer: going from one place to another, port from porter: to carry) turned to be more than an ID document, they also confirmed that the holder was member of the issuing State and thus accepted as citizen and protected by it. Especially the issuing State allowed the travelling, including return and reintegration in the State of origin after return.

Though the 19th century also is called the passport-less century – most States in middle and western Europe cancelled the obligation to carry a passport in the last third of this century –, a number of different regulations on ID documents and citizens' registration remained.[11]

In the past century ID cards came to be introduced. In the First World War (1914-1918) in Germany an ID card was introduced, as in times of war, control of people moving around and their identification seemed to be very important. Originally it was planned to have fingerprints in this ID card, but this was not implemented as dactyloscopy (comparison of fingerprints) typically was used as a forensic method at that time, replacing the anthropometria (registration and comparison of physical properties of persons).

At that time the German State decided to use photos in ID cards in order not to convey the impression that the ID card holder might be a criminal.[12] In the 1930s in Germany a national ID card (so called Kennkarte) was established.

Currently national ID documents and passports are changing their character, as smart chips, RFID chip, magnetic stripes or laser engraved zones (a so-called laser band) are increasingly introduced. They are used to store information about the holder of the ID document digitally. In fact digital storage, transfer and processing of identifying information become increasingly important.

One example of this is credit cards which also can be used for payment purposes via the internet. In the USA where currently no national ID card exists, the credit card also is used for identification purposes, e.g., in hotels or when booking a flight. In fact in Anglo-American countries national ID documents never were really established except in times of war.

3 Legal aspects

Taking the needs of eGovernment as a starting point, the legal contribution to the study discusses the roles so-called entities can have in a particular sector. Entities can be attributed a global, sector-specific or context specific identifier. In e-government an attempt is made to optimise service delivery by channelling internal and external relationships through technology.

Interoperability and the usage of common ID numbers for all relevant entities then make the usage of ID numbers tantamount for e-government. Bearing this in mind the question is whether they are supported by a sound legal framework, whether the usage of global identifiers is enough to guarantee the rights of the individual as defined in the European Data Protection Directive[13] or should technical unlinkability also be a requirement of e-government architecture?

The contribution makes clear that ID numbers are personal data and therefore the processing of these numbers should be carried out subject to the Data Directive. This means that attention should be given to the legitimacy of the processing, the data quality and aspects of confidentiality and security. It may be said to be unfortunate that the Directive leaves the standards for safeguards for ID-numbers, that Member states put in place, up to the Member states.

With the present state of knowledge it might have been expected that due to the value the Directive puts on the sound protection of the ID number, that technical unlinkability would have been prescribed. After all, the Directive does point out that appropriate technical and organisational security measures must be taken. These should take account of the state of the art, the cost of their implementation and the risks represented by processing and the nature of the data.

In the context of eGovernment the processing of personal data should be respecting the minimum data and data processing quality principles, such as the 'finality' and the 'proportionality' principle (article 6 of the Directive).

Briefly summarized, the term *finality* refers to the obligation to only collect personal data for specified, explicit and legitimate purposes. Personal data shall not be further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible if the appropriate safeguards are taken. The purpose of the processing should be defined the latest at the moment of the collection of the data.

10 Probably for this reason many VIPs think that a request for identification comes close to an offence (Wesel, *Geschichte des Rechts,* 1997).

11 Gosewinkel, D., Einbürgern und Ausschliessen, Göttingen, 2001.

12 Donatsch, A., Identifizierung von Tatverdächtigen in: Unipublic., Veröff. Der Universität Zürich, 2000.

13 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *Official Journal of the European Communities,* L 281, 23 November 1995, pp. 31 – 50.

The *proportionality* principle has to be understood in terms of:

- storage duration: The processed data may not be kept in a form permitting identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- necessity of the data: The processed data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.
- further processing of the data: The purposes of further processing should not be incompatible with the purposes initially defined for which the data were collected.
- accuracy: personal data should be accurate and, where necessary, kept up to date.

Applied to ID numbers, it is clear that the data controller that decides to make use of a global, sector-specific or context-specific identifier should:

- make sure that the chosen data (for example, a global ID number instead of a sector-specific one) is adequate, relevant and not excessive in relation to the purposes for which it is being collected and/or further processed;
- make sure that the ID number is accurate and, where necessary, kept up to date and
- not kept in a form which permits identification of data subjects longer than is necessary for the purposes for which the data were collected or for which they are further processed.

In addition, on the topic of finality and proportionality, it is important to note that when two or more government entities integrate their back-offices, there will typically be a reuse of personal data for another purpose than the one that was originally indicated.

For example, when a particular set of data has been collected from a citizen for unemployment allowance purposes, the idea of eGovernment would be to make that data directly available to the tax authorities – of course within the borders of the law – instead of asking it again to the citizen.

As mentioned, the finality principle requires the further processing to be compliant with the original purposes.[14]

The main point of departure is that identifiers are definitely needed in the public sector, especially to achieve the goals of eGovernment, for instance, "the integration of back-offices". Without data protection rules, it seems obvious to choose common, global identifiers between these back-offices, and not technically to be constrained by context- and or sector-specific identifiers.

The question that is raised is whether the usage of global identifiers within a sound legal framework can be acceptable from a legal perspective for the default data exchange between two or more government entities or not. The alternative would be to choose technical unlinkability as a requirement of an eGovernment architecture, which would imply the usage of context- and/or sector-specific identifiers.

At the other side of the spectrum, the study analyses the data protection rules. From this perspective, the conclusion was drawn that:

- If the usage of global identifiers is forbidden in the Member State (e.g., because it is unconstitutional), technical unlinkability should be a requirement of the architecture design.
- The Data Protection Authority has the important task of verifying that context-specific numbers are indeed not being used outside their respective contexts.
- If the usage of *some or all* global identifiers is regulated, the basic data protection rules still apply. The additional rules should take the data protection principles as a minimum. The Data Protection Authority here mainly verifies whe-

14 For instance, this means that it is absolutely unacceptable for a bank to process client payment data for direct marketing purposes. This further processing is here clearly incompatible with the original purposes.

ther the conditions under which that identifier may be processed are fulfilled.
- If the usage of global identifiers is allowed or at least is not forbidden, the Data Protection Authority only verifies whether the number is being processed within the limits of the data protection regulation (finality, proportionality, protection level etc.), as explained above.[15]

Additional, crucial issues were noted, when having a closer look at the data protection principles. From this analysis it can be indicated that:
- The data controller should make sure that the chosen data (for example, a global ID number instead of a sector-specific one) is adequate, relevant and *not excessive* in relation to the purposes for which it is being collected and/or further processed.
  In other words, a global identifier can be excessive in relation to the purposes for which the data is being collected. For instance, if no legitimate cross-context or cross-sector data exchange is present at the first processing of the ID number, a context- or sector-specific identifier should suffice.
- The data controller should make sure that the ID number is not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- In practice, this means that when the purposes of processing the ID number have been realised, it should be anonymized. Encrypting or encoding the ID number will most probably not be sufficient if the reason why the ID number is being processed like that (encrypted …) is to be able to re-identify the person if needed. In that case, the ID number would still be identifiable data – and thus also personal data.
- To evaluate the necessary, "appropriate" technical and organizational security measures, three factors play a role: (1) the state of the art, (2) the cost of their implementation and (3) the risks represented by the processing and the nature of the data to be protected.

The state of the art means that security measures should follow the technological evolution. This means that if technologies to ensure unlinkability between contexts and sectors mature sufficiently (which is more and more the case today) they should be chosen if they are more conducive towards achieving the goals of the processing. It also means that it can be an unacceptable risk to not take unlinkability measures.

Yet, this is also the tricky part of the answer to the above mentioned question on "technical unlinkability": it depends on the evaluation of the case at stake.

The technical section of the study shows that, unfortunately, the present legal framework soon becomes inadequate in preventing the technical linkability of potentially privacy harmful data about citizens on the basis of ID numbers. Once the necessary infrastructure is in place, including global ID numbers, data exchange will take place anyway either legitimately or illegitimately, based on an ad hoc argument or on political choices.

4 Sociological aspects

In spite of the many managerial advantages, ID numbers arouse strong emotions which cannot be solely comprehended from a legalistic suspicion of being potentially harmful to the individual's privacy. Therefore the study introduces a sociological analysis of the function of ID numbers. The sociological approach is looked at from two angles: social systems theory and a theory on the role of bureaucracy in national states.

The social systems theory views society from a general perspective, allowing the analysis of the function of ID numbers in private and public organisations. By thoroughly analysing the function of names, identifiers and addresses it can be ascertained that ID numbers fulfill all three functions of a name, an identifier or an address. First, they can be used as names for a data set or a number of data sets in a database. Secondly, they can be used as identifiers if they link a person uniquely in an administrative context. Thirdly, they can also be used as addresses. In the organisational context, social systems theory learns that addresses are always administered (generated, assigned and deleted or deactivated) by organisations. Organisations also are also careful to resolve potential address collisions by keeping addresses unique in the particular scope of the operation. The state ensures addressability for governmental, private-sector or interactional (citizen to citizen) operations. Addressability today covers persons, families, organisations and objects in the context of communication techniques. Addressability is not possible without organisations. These organisations need the unique identifiability to run their operations smoothly and efficiently. This in turn may lead to information asymmetry because, as shown in the legal analysis, it reduces the autonomy of individuals by the usage of linkability measures. In other words, a shift of power may occur in favour of the organisation. In the context of states in many cases it is difficult to decide whether citizens overall benefit from this development or not, the reason being that citizens typically take on two roles with respect to the state. On the one hand they are members and thus benefit from a strong state that is able to protect them and, on the other hand they are clients of the state who suffer from reduced autonomy.

The second sociological angle is based on the Weberian theory of bureaucracy. Against the background of the rationalisation processes going on in all areas of society, the function of ID numbers is described as having the purpose of providing the members of a state with a feeling of unity and cohesion within the perspective of increased globalisation. It can be said that in the past political rationalisation resulted in the formalisation of the state.

One of the unique properties of a state is a trained corps of civil servants specially trained in and restricted to regulations. This corps of civil servants has as its main task, the identification of the members of the state to enable the state to carry out its primary tasks. According to Weber these bureaucracies are the ultimate example of the rationalisation process because they aim at efficiency, predictability, quantifiability, control by substituting human judgement by non-human technology and irrationality by rationality.

To carry out its tasks the bureaucratic government accordingly issued identity cards and codes. These identification means provided access to a whole series of files and data sets. ID numbers therefore became the symbols of this bureaucratic

15 De Bot, D., Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart, [Privacy protection in e-government in Belgium. A critical analysis of the Rijksregister, the Crossroads bank of enterprises and the electronic identity card] Vandenbroeke, Brugge, 2005, p. 56.

culture. Seemingly meaningless numbers acquire meaning in this bureaucratic context because the developing nation-states desired to attach meaning to this symbol.

Sociologically speaking it is argued, this was an unfortunate choice because, as Weber already pointed out, this was the irrationality of rationality. The intention of creating a notion of unity and solidarity was not attained because citizens felt, that the ID number identification led to depersonalisation. It could be argued, that the mismanaged effort to create unity in states by the introduction of the ID-number, actually led to a sense of loss of privacy without contributing to the sense of unity.

5 Technical aspects

Taking the risks and opportunities of ID-numbers in the modern technological age, an investigation is made of the contrast between requirements that techniques such as profiling pose vis-à-vis the protection of the individual's privacy privileges. Profiling provides a new kind of knowledge used for decision-making based on Knowledge Discovery in Databases (KDD). KDD requires per definition as much information as possible about the individual, whereas traditional privacy rights focus on data minimisation. There is no easy solution for this conflict.

One approach is to ask citizens to be more transparent by introducing sector-wide and unique ID numbers, while at the same time attempts are made to make the state and its actions more transparent. Examples are, in the Netherlands, the introduction of the National Trust Function to log the use of the national ID number and, the introduction of Freedom of Information Acts in Germany, allowing citizens to access their own data files maintained by the state.

Unfortunately, these attempts fall short in certain cases. In addition to limitations for citizens to access secret data, which is very understandable because these could be covered by trust based models, the use of profiling creates additional limitations for transparency. Certain types of profiles are not linked to the data they were derived from, they are no longer personal data and, may be used to the disadvantage of the citizen in a non-transparent way.

Due to the complexity of the underlying profiling processes, regulatory attempts to increase transparency fall short and, Transparency Enhancing Technologies (TETs) to fill this gap are limited in effectiveness or do not even exist yet. Another problematic aspect of transparency is that from a social perspective people think, communicate and act in communicational terms. Data freely used in one context cannot necessarily be used in another.

Keeping data in its appropriate context is also called the concept of contextual integrity. Informational self-determination can be understood as an important attempt to put contextual integrity in legal norms, though certainly from a social perspective an inappropriate one in certain cases. These aspects are further elaborated in the FIDIS deliverable D7.9.[16]

Yet another approach is the introduction of additional functions and tools that make the individual less recognisable or opaque. In this context different methods have been developed and implemented to restrict and control linkability facilitated by ID numbers. On the whole the technical study arrives at the conclusion that by introducing the concepts of contextual integrity and reciprocal transparency in combination with multiple identifiers, it looks like that both the needs of KDD techniques as well as the concept of privacy can be achieved. This does need a fine-tuned combination of transparency and opacity tools to be built into the new technogical infrastructure.[17]

6 European approaches

The report gives an empirical study of the background and present policy and usage of ID numbers in a sample of various EU countries. An attempt is made to provide an overview that shows how the attitudes towards and the choices made with respect to the usage of ID numbers can be very different in the EU region.

For this reason country reports have been included on Belgium, France, The Netherlands, Czech Republic, Slovak Republic, Hungary, Germany, Switzerland and Austria.

These country reports illustrate how the conceptual aspects that are analysed earlier are put into practice. These empirical and conceptual approaches make it possible to elicit lessons learned and provide benchmarks, by which to develop arguments for policy recommendations.

Taking into account national political strategies and existing infrastructures four different basic concepts on how to deal with ID numbers can be determined from the country reports. They are:

1. Introduction of sector spanning ID numbers with a large area of use inside and outside the public sector mainly based on mutual transparency of use (example: The Netherlands)
2. Introduction of sector spanning ID numbers with regulations on how they may be used (examples: Switzerland, Czech Republic and Slovakia)
3. Introduction of sector specific ID numbers and organisational enforcement of borders of sectors (examples: Hungary, France, Germany)
4. Introduction of sector specific ID numbers and organisational as well as technical enforcement of borders of sectors (example: Austria)

7 Conclusions

The analysis of ID-numbers and policies as provided in this Fidis study shows that ID-numbers are an essential tool for the realisation of eGovernment and modern business processes. Due to the increasing pervasiveness of Internet as a means of communication by governments and enterprises, there is a growing necessity for a secure identity management.

The need to identify who communicates with whom is essential in an Internet environment because the Internet, by design, lacks these provisions. Because of these shortcomings various solutions have been developed.

The identity number is a prominent one. As is shown, the developments in this area could affect the privacy interests of individuals. Individuals often need to disclose more personal data than strictly re-

16 Hildebrandt, M. and Koops, B.J. (eds.), D7.9: A vision of ambient law, FIDIS Deliverable, 2007.

17 Gutwirth, S. and De Hert, P., 'Privacy and Data Protection in a Democratic Constitutional State. Profiling: Implications for Democracy and Rule of Law', in Hildebrandt, M., Gutwirth, S. and De Hert P. (eds.), D7.4: Implications of profiling practice on democracy, FIDIS Deliverable, 2005.

quired.[18] Several steps are still being taken to tackle this problem.[19]

The sociological and the historical analyses indicate that only a carefully attuned policy will allow the present possibilities and opportunities of ID-numbers to be used successfully. From the socio-cultural point of view, experiences in using the identification tool as a method by which to create a feeling of unity in a nation-state, that only exists in the minds of the heads of state, have led to the opposite result.

From the social systems point of view, there are potential benefits as well as drawbacks in the usage of an ID-number. In the public domain one of the drawbacks could be caused by the fact that citizens are members of a state as well as clients. The state benefits from the advantages of using ID-numbers and therefore these benefits also are beneficial to its members.

Drawbacks might arise when these measures harm the clients of organisations when ID-number linkability is used to create information asymmetry in favour of organisations. Organisations may use this asymmetry to reduce the autonomy of the individuals. This, in turn, may result in a shift in the balance of power favouring organisations.[20]

The potential information asymmetry, as achieved by technical means, is illustrated by describing profiling techniques. Even though there are the large risks of abuse in these scenarios, the suggestions for making good use of the opportunities technology has to offer are promising.

This privacy-friendly scenario can be achieved through a joint effort of computer engineers, legal experts and policymakers. Within the scope of the European Data Directive the opportunities for using profiling techniques can thus be put to good use. Individuals can then be monitored without necessitating any kind of transcontextual identification. This fits in with the purpose of the limitation principle of the Directive.

Without a doubt, the protection of personal data is a fundamental right in the European Union. In many Member States it is a constitutional right.[21] However, if appropriate attention is given to the rights of individuals such as is expressed in the legitimacy of the processing, the data quality and aspects of confidentiality and security and the principle of the protection of personal data or so-called informational privacy, this will enable a sound identity management. In the area of profiling this seems to call for limiting the use of personal data to the proper context. However, this could preclude the use of profiling to its full potential.

It may be instrumental to redefine the concept of privacy in terms of "privacy as contextual integrity"[22] while, at the same time, underpinning it with the appropriate technical means. In this light it seems preferable and feasible to adopt multiple ID-number policies.

These allow to discriminate between different contexts providing tailored ID-number policies, depending on which type of privacy is appropriate per context. The point of departure is a type of identity management based on user control. At the same time, the reciprocity or distribution of the transparency can be tailored, depending on the need for checks and balances per context.

This does not necessarily rule out interoperability between contexts, because ID-numbers may be linked, e.g. via clearing houses, to provide interoperability. The information asymmetry that looms behind the horizon may thus lead to the sought for sensible use of the ID number with due respect for the privacy of the citizens concerned.

In essence it may be concluded that multiple identifiers in conjunction with interoperability and contextual integrity are the most promising solution for a sound identity management policy in the near future. This requires a fine-tuned combination of transparency and opacity tools to be built into the technological infrastructure.

In such a way the individual will not become unnecessarily transparent nor will interoperability be precluded by excessive user control. The advantages of eGovernment can thus be achieved reciprocally for government and citizen alike. Measures to prevent identity fraud must be part of this IDM policy while, at the same time, the corresponding security measures must be construed in such a way as to inspire the citizen with sufficient trust that the government treats his data safely.

It may not be an unrealistic assumption that, if this avenue of using technology in this constructive way is followed, the concerns, that arose from the analysis of the several constitutive elements of ID number policy choices, can be sufficiently addressed.

18 Cf Koops, B.J., Buitelaar, H. and Lips, M. (eds), D5.4: Anonymity in electronic government: a case-study analysis of governments' identity knowledge, FIDIS Deliverable, 2007.

19 Cf among other things the work done by the PRIME consortium as set out in the PRIME white paper v2, 27 June 2007.

20 Bygrave, L.A., Data Protection Law, Approaching its rationale, logic and limits, Kluwer Law International, The Hague, London, New York, 2002, pp. 94-95 writes "Public concern over such schemes centred primarily on their potential to significantly roll back the privacy and autonomy of citizens and undermine in turn the foundations for democratic, pluralistic society." This is even more harmful.

21 The Charter of Fundamental Rights of the European Union enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7 thereof and the same is the case at national level in some states. Cf Opinion 4/2007 of 20th June 2007 of the Article 29 Data Protection Working Party on the concept of personal data, available at http://ec.europe.eu/justice_home/fsj/privacy/workinggroup/index_en.htm, p.7.

22 A concept introduced by H. Nissenbaum in Nissenbaum, H., 'Privacy as Contextual Integrity', Washington Law Review 79, 2004, pp. 101-140.